LARA LICENSING AND REGULATORY AFFAIRS CUSTOMER DRIVEN. BUSINESS MINDED.	**Effective Date:**	09-12-2011
	Policy #:	G-17
	Supersedes:	
Subject: **Information Privacy and Security**	**Page:**	1 of 4

PURPOSE

The Department of Licensing and Regulatory Affairs (LARA) administers programs with a wide range of personal information. In fulfilling these duties, the department must use, maintain, and safeguard sensitive personal data. This policy protects and preserves the internal and external information sharing requirements.

This policy establishes a common understanding of information security based on the principles of confidentiality, integrity, and availability. Confidentiality limits information access to authorized users. Integrity protects information against unauthorized modification. Availability ensures that information is accessible when needed. Together, these principles ensure the information can be used to properly provide services to our clients. The department expects information and related assets to be accurate, available for authorized use, and protected from misuse or modification.

DEFINITIONS

Department Information - All information used by the department or its workforce to conduct department business.

Department Records - Recorded information, in any form, created or received in conducting department business and kept as evidence of such activity, excluding transitory work products.

Data Handling - Using, storing, processing, transferring, administering, aggregating, sharing, and maintaining department information

Information Security - Protecting the confidentiality, integrity, and availability of department information.

Information Technology Assets - ***Applications***, computer systems, servers, networks, and related devices owned by or entrusted to the department.

Security Classifications - Categories of department records based upon intended use and expected impact if disclosed.

- **Public** — Records disclosable without redaction under Freedom of Information Act requests that, when used as intended, would have minimal or no adverse effect on the operations, assets, or reputation of the department or its obligations concerning information privacy.
- **Restricted** — Records intended for internal use within the department that, if disclosed, could be expected to have a serious adverse effect on the operations, assets, or reputation of the department or its obligations concerning information privacy. Restricted data may include data implicating operational concerns rather than individuals' privacy concerns. The release or disclosure of restricted data should only occur consistent with existing redaction, de-identification, and other privacy policies.
- **Sensitive** — Records intended for limited internal use within the department that, if disclosed, could be expected to have a severe adverse effect on the operations, assets, or reputation of the department or its obligations concerning information privacy. Sensitive data may include data connecting a person's name with the person's (a) social security or driver's license number, (b) medical information, (c) financial information, or (d) other information designated as sensitive by the Privacy Council. The release or disclosure of sensitive data should only occur consistent with existing redaction, de-identification, and other privacy policies.

Workforce - Employees, staff from third-party entities, and others authorized to perform work for the department.

SCOPE

This policy applies to department staff, contractors, and all others granted use of department information or related assets and defines their responsibility to protect and appropriately use department information, applications, computer systems, and networks. This policy provides general standards for handling department information in written and electronic formats. The Department of Technology, Management and Budget (DTMB) also is responsible for security for computer systems used by the department's workforce.

Compliance with relevant Department of Technology, Management and Budget (DTMB) Administrative Guide and DTMB security standards is also mandatory, when applicable. These standards include, but are not limited to, the following:

- DTMB Information Technology Standards and Planning Procedures

In addition to these general policies, specific department systems and work areas with elevated security risks or legal mandates operate under additional security procedures. These include Health Insurance Portability and Accountability Act (HIPAA) policies and security and access policies governing HRMN and MI-HR staff. Each work area with such special requirements shall designate a Data Steward. The Data Steward is responsible for ensuring the security of the relevant information and coordinates with the Information Privacy Officer to ensure department-wide compliance with all relevant standards. Department staff assigned to other departments also must comply with relevant policies of their host agency.

ORGANIZATION

The Department of Licensing and Regulatory Affairs (LARA) Information Privacy Officer (IPO) within the Director's Office shall oversee the information security policy for the department. The IPO will coordinate the assignment of applicable information to one of three security classifications: public, restricted, or sensitive. These classifications are based upon the information's intended use, individuals' privacy interests in the information, and the expected impact if disclosed. Bureaus shall summarize in writing any additional procedures regarding information security for data that they oversee.

The Information Privacy Officer and DTMB Liaison shall oversee these policies and standards and shall specify controls to manage risks to the confidentiality, integrity, and availability of department information and related assets. All LARA workforce members must comply with these controls.

The department shall conduct periodic risk assessments to determine the effectiveness of such controls and perform audits to measure compliance. The department will provide information to all members on the proper use and disclosure of personal identifying information as appropriate to each bureau, agency, commission or office.

The LARA Director's Office and DTMB will review information technology product or service contracts. This review will include identification of risks related to information security. The department complies with all applicable legislative, regulatory, and contractual requirements concerning information security. Department information security standards may exceed legally prescribed requirements.

ENFORCEMENT

The IPO will investigate suspected violations, and may recommend discipline in accordance with department rules, regulations, and policies or applicable laws. Sanctions may include the following:

- Suspension or termination of access
- Discipline, up to and including dismissal
- Civil or criminal penalties

Reporting Violations

All department workforce members must report suspected violations of this policy to the IPO and the appropriate bureau director. Reports of violations are considered sensitive information and are treated confidentially.

REFERENCES

National Institute of Standards and Technology – Guide to Protecting the Confidentiality of Personally Identifiable Information
http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf